Birch Swinnerton-Dyer予想に関するKolyvaginの仕事の紹介(代数的整数論と数論的幾何学)

AUTHOR(S):

青木, 昇

CITATION:

青木, 昇. Birch Swinnerton-Dyer予想に関するKolyvaginの仕事の紹介(代数的整数論と数論的幾何学). 数理解析研究所講究録 1995, 925: 10-18

ISSUE DATE:

1995-10

URL:

http://hdl.handle.net/2433/59813

数理解析研究所講究録
925巻 1995年 10-18

Birch Swinnerton-Dyer 予想に関する Kolyvagin の仕事の紹介

立教大学理学部　青木　昇

1 Birch Swinnerton-Dyer 予想

有理数体上定義された楕円曲線

$$E : y^2 = x^3 + Ax + B \quad (A, B \in \boldsymbol{Q})$$

を考える。一般に有限次代数体 k に対して、Mordell-Weil の定理により $E(k)$ は有限生成であるから

$$r(E/k) = \mathrm{rank} E(k)/E(k)_{\mathrm{tor}}$$

は負でない整数である。更に、$L(E/k, s)$ を E/k の L 関数とする。以下において、Hasse-Weil 予想は常に成り立つものとする。そこで、

$$\rho(E/k) = \mathrm{ord}_{s=1} L(E/k, s)$$

とおくと、これは負でない整数である。

ここでは $k = \boldsymbol{Q}$ または虚二次体 $K = \boldsymbol{Q}(\sqrt{D})$ の場合について Birch Swinnerton-Dyer 予想（以下 (BSD/k) と略記する）を考える。そのために、Tate-Shafarevich 群 Ш(E/k) を次のように定義する。

$$Ш(E/k) = \ker \left(H^1(k, E) \longrightarrow \prod_{v \in \Sigma_k} H^1(k_v, E) \right)$$

ここで Σ_k は k の素点の集合を表わす。先ず、$k = \boldsymbol{Q}$ の場合 (BSD/$\boldsymbol{Q}$) は次のように述べられる。

$(BSD(1)/Q)$ $\qquad r(E/\boldsymbol{Q}) = \rho(E/\boldsymbol{Q}) \qquad (= r \text{ とおく})$

$(BSD(2)/Q)$ $\qquad \lim_{s \to 1} \dfrac{L(E/\boldsymbol{Q}, s)}{(s-1)^r} = \dfrac{\det(\hat{h}(P_i, P_j))|\ Ш\ (E/\boldsymbol{Q})|}{(E(\boldsymbol{Q}) : \sum \boldsymbol{Z} P_i)^2} \cdot \prod_{p|N} c_p \cdot \Omega$

ここで $P_1, \cdots, P_r$ は $E(\boldsymbol{Q})$ の $\boldsymbol{Z}$ 上独立な元である。他の記号については中島氏の論説を参照されたい。

次に、$k = K$ の場合について考える。全く一般の場合を考えるのは大変なので、K が次の条件を満たすとしよう。

(K) $\qquad (|D|, 2N) = 1, \qquad D \equiv \text{ square } (\mathrm{mod}.4N).$

このとき E/K に対する (BSD/K) は次のようになる。

$(BSD(1)/K)$ $\qquad r(E/K)=\rho(E/K) \qquad (=r \text{ とおく})$

$(BSD(2)/K)$ $\qquad \lim_{s\to 1}\dfrac{L(E/K,s)}{(s-1)^r}=\dfrac{\det(\hat{h}(P_i,P_j))|\text{Ш}(E/K)|}{(E(K):\sum \boldsymbol{Z}P_i)^2}\left(\prod_{p|N}c_p\right)^2\Omega\Omega'$

ここで $P_1,\cdots,P_r$ は $E(K)$ の $\boldsymbol{Z}$ 上独立な元である。$K/\boldsymbol{Q}$ に関する E の twist を

$$E': Dy^2=x^3+Ax+B$$

とするとき Ω' は E' に対する period である。

もし $E/\boldsymbol{Q}$ と $E'/\boldsymbol{Q}$ に対する (BSD(1)/$\boldsymbol{Q}$) が成り立てば E/K に対する (BSD(1)/K) も成り立つ。実際、それは次の関係式より明らかである。

$$\begin{aligned} r(E/K) &= r(E/\boldsymbol{Q})+r(E'/\boldsymbol{Q}) \\ \rho(E/K) &= \rho(E/\boldsymbol{Q})+\rho(E'/\boldsymbol{Q}) \end{aligned}$$

(BSD/K) についての Gross と Zagier の結果を述べるために次の条件を考える。

(M) $\qquad E$ は modular である。

ここで E が modular であるとは、有理数体上定義された自明でない morphism $\varphi: X_0(N)\to E$ で $\varphi(i\infty)=0$ となるものが存在することである。

Theorem 1.1 (Gross-Zagier, [2]) 条件 (K)(M) の下で次が成り立つ。

$$L'(E/K,1)=\frac{\hat{h}(y_K)}{(cu_K)^2}\Omega\Omega'.$$

ここで u_K は K 内の 1 の巾根の数の $\frac{1}{2}$ を表わし、$y_K\in E(K)$ は *Heegner point* と呼ばれる点（次節を参照）である。

さて、(K) の下では $\rho(E/K)$ は奇数であることが判る。従って特に $\rho(E/K)\geq 1$。よって Theorem 1.1 より $\rho(E/K)=1$ と $h(y_K)\neq 0$ は同値であるが、これは y_K が無限位数であることと同値である。そこで、条件

(H) $\qquad y_K$ は無限位数である。

を考えると、次が成り立つ。

Corollary 1.2 (K)(M) の下で、$\rho(E/K)=1$ であることと (H) は同値である

更に、次のことが成り立つ。

Corollary 1.3 条件 (K)(M) の下で次が成り立つ。
(i) E に対して (BSD(1)/K) が成り立つことと $r(E/K)=1$ は同値である。
(ii) E に対して (BSD(2)/K) が成り立つことと次は同値である。

$$|Ш(E/K)| = \left(\frac{(E(K):\boldsymbol{Z}y_K)}{cu_K\prod c_p}\right)^2$$

(証明) (i) は Corollary 1.2 より明らか。(ii) は (BSD(2)/K) の式と Gross-Zagier の式を比べることにより従う。□

Kolyvagin は次の定理を証明した。

Theorem 1.4 条件 (M)(K)(H) の下で、$r(E/K)=1$ である。(従って E に対して (BSD(1)/K) が成り立つ。) 更に、$Ш(E/K)$ は有限群である。

(BSD(2)/K) について Kolyvagin は $|Ш(E/K)|$ の評価式を与えている。それを述べるために素数 p に対する次の条件を考える。

$(G(p))$ $$\mathrm{Gal}(F(E_p)/F)\cong \mathrm{Aut}_{\mathcal{O}}E_p$$

ここで、$\mathcal{O}=\mathrm{End}E$ であり、F は $\mathcal{O}$ の商体を表わす。

Theorem 1.5 条件 $(G(p))$ の下で次が成り立つ。

$$\mathrm{ord}_p|Ш(E/K)| \le 2\mathrm{ord}_p(E(K):\boldsymbol{Z}y_K)$$

実際には Kolyvagin はすべての素数に対して $|Ш(E/K)|$ の評価を与えている。しかし、条件 $(G(p))$ なしでは定理のようにきれいな評価式は得られていない。

2 Heegner points

以下では常に条件 (K)(M) を仮定する。従って、有理数体上定義された morphism

$$\varphi : X := X_0(N) \longrightarrow E, \quad \varphi(i\infty)=0$$

が与えられている。さて、自然数 n に対し $\mathcal{O}_n$ を conductor n の $\mathcal{O}_K$ の order とし、$\mathfrak{n}$ を $\mathcal{O}_n$ のイデアルでノルムが N となるものとする。(こういうイデアルの存在は条件 (K) により保証されている。) このとき、二つの楕円曲線の間の cyclic N-isogeny $\boldsymbol{C}/\mathcal{O}_n \to \boldsymbol{C}/\mathfrak{n}^{-1}$ は $X(\boldsymbol{C})$ 上の点 x_n を定める：

$$x_n = (\boldsymbol{C}/\mathcal{O}_n \to \boldsymbol{C}/\mathfrak{n}^{-1}) \in X(\boldsymbol{C}).$$

K_n を K 上の conductor n の ring class field とすると、虚数乗法論より $x_n \in X(K_n)$ であることがわかる。更に、

$$\begin{aligned} y_n &= \varphi(x_n) \in E(K_n) \\ y_K &= \mathrm{Tr}_{K_1/K}(y_1) \in E(K) \end{aligned}$$

とおく。前に述べたように、$y_K \in E(K)^{\varepsilon} + E(K)_{\mathrm{tor}}$ である。

p を奇素数で条件 $(G(p))$ を満たすものとし、以下固定する。NDp を割らない素数全体を Λ_1 で表わす。更に、自然数 M に対し Λ_1 の部分集合

$$\Lambda_1(M) = \{\ell \in \Lambda_1 \mid \mathrm{Frob}(\ell) = \mathrm{Frob}(\infty) \text{ in } K(E_{p^M})\}$$

を考える。ここで $\mathrm{Frob}(\ell)$ と $\mathrm{Frob}(\infty)$ はそれぞれ ℓ と複素共役の $\mathrm{Gal}(K(E_{p^M})/\boldsymbol{Q})$ における共役類を表わす。従って、素数 $\ell \in \Lambda_1$ が $\Lambda_1(M)$ に属するためには次の二つの条件が成り立つことが必要十分である：

- ℓ は $K/\boldsymbol{Q}$ で remain prime である。(それを λ と表わす。)
- λ は $K(E_{p^M})/K$ で完全分解。

更に、$\mathrm{Frob}(\ell)$ と $\mathrm{Frob}(\infty)$ の $E_{p^M} \cong (\boldsymbol{Z}/p^M\boldsymbol{Z})^2$ への作用を考えたときの固有多項式を比べることにより、この条件は次と同値であることが判る。

- $\ell + 1 \equiv a_\ell \equiv 0 \pmod{p^M}$.

さて、$r \geq 1$ に対して

$$\Lambda_r(M) = \{n = \ell_1 \cdots \ell_r \mid \ell_i \in \Lambda_1(M),\ \ell_i \neq \ell_j\ (i \neq j)\}$$

とおく。便宜上 $\Lambda_0(M) = \{1\}$ とし、

$$\Lambda(M) = \bigcup_{r \geq 0} \Lambda_r(M)$$

とおく。また、$n \in \Lambda(M)$ に対し

$$G_n = \mathrm{Gal}(K_n/K_1)$$

とおくと $\ell \in \Lambda_1(M)$ に対しては G_ℓ は位数 $\ell + 1$ の巡回群である。各 ℓ にたいしてその生成元 σ_ℓ を固定しておく。一般の $n \in \Lambda(M)$ に対しては

$$G_n \cong \prod_{\ell \mid n} G_\ell$$

更に、$\mathcal{G}_n = \mathrm{Gal}(K_n/K)$ とおく。

以下において重要になる E 上の点列 $\{P_n \in E(K_n)\}_{n\in\Lambda(M)}$ を定義しよう。そのために Kolyvagin operator D_n を次のように定義する。まず、$\ell \in \Lambda_1(M)$ に対し

$$D_\ell = \sum_{i=1}^{\ell} i\sigma_\ell^i \quad \in \boldsymbol{Z}[G_\ell]$$

とおき、次に $n \in \Lambda(M)$ に対して

$$D_n = \prod_{\ell|n} D_\ell \quad \in \boldsymbol{Z}[G_n]$$

とおく。この D_n と上で定義した y_n を用いて $P_n \in E(K_n)$ を

$$P_n = \sum_{\sigma\in\mathcal{G}_n/G_n} \sigma(D_n y_n)$$

により定義する。特に $P_1 = y_K$ であることに注意する。この P_n に対して

$$\mathrm{ord}_p P_n = \sup\{m \in \boldsymbol{Z} \mid P_n \in p^m E(K_n)\} \leq \infty$$

とおく。P_n が無限位数ならば $\mathrm{ord}_p P_n < \infty$ である。$r \geq 0$ に対して

$$M_r = \min\{\mathrm{ord}_p P_n \mid n \in \Lambda_r(\mathrm{ord}_p P_n + 1)\}$$

とおく。特に、$M_0 = \mathrm{ord}_p P_1$ である。このとき次が成り立つ。

Proposition 2.1 条件 $(G(p))$ の下に次が成り立つ。(i) y_K が無限位数ならば $M_0 = \mathrm{ord}_p(E(K) : \boldsymbol{Z}y_K)$.

(ii) $M_0 \geq M_1 \geq M_2 \geq \cdots$.

(証明) $(G(p))$ が成り立てば、$(n, NDp) = 1$ なる 任意の n に対して $E(K_n)_p = 0$ であることが知られている ([1], Lemma 4.3)。

(i) まず、$E(K_1)_p = 0$ より自然な写像

$$E(K)/p^M E(K) \longrightarrow E(K_1)/p^M E(K_1)$$

は単射であることがわかる。実際、この写像の kernel は $E(K) \cap p^M E(K_1)/p^M E(K)$ であるが、$P \in E(K) \cap p^M E(K_1)$ に対し $P = p^M Q$ なる $Q \in E(K_1)$ をとると、任意の $\sigma \in \mathrm{Gal}(K_1/K)$ に対し $p^M(Q^\sigma - Q) = 0$ である。ところが、$E(K_1)_p = 0$ であるから $Q^\sigma = Q$。従って、$Q \in E(K)$ となり $E(K) \cap p^M E(K_1) = p^M E(K)$ が判る。

(ii) の証明は略す。([7], Lemma 5.1 を参照。) □

Theorem 2.2 条件 (K)(M)(H)$(G(p))$ の下で、

$$Ш(E/K)_{p^\infty}^{-\varepsilon} \cong \left(\boldsymbol{Z}/p^{M_0-M_1}\boldsymbol{Z}\right)^2 \oplus \left(\boldsymbol{Z}/p^{M_2-M_3}\boldsymbol{Z}\right)^2 \oplus \cdots.$$
$$Ш(E/K)_{p^\infty}^{\varepsilon} \cong \left(\boldsymbol{Z}/p^{M_1-M_2}\boldsymbol{Z}\right)^2 \oplus \left(\boldsymbol{Z}/p^{M_3-M_4}\boldsymbol{Z}\right)^2 \oplus \cdots.$$

この定理より定理 1.5 が従う。実際、$m = \min\{M_r \mid r \geq 0\}$ とおくと

$$\mathrm{ord}_p |Ш(E/K)| = 2(M_0 - m) \leq 2\mathrm{ord}_p(E(K) : \boldsymbol{Z}y_K).$$

3 Selmer 群と Euler system

F を K の任意の拡大体とし、descent sequence

$$0 \longrightarrow E(F)/p^M E(F) \xrightarrow{\delta_F} H^1(F, E_{p^M}) \xrightarrow{j_F} H^1(F, E)_{p^M} \longrightarrow 0$$

を考える。$F = K_v$ $(v \in \Sigma_K)$ のときは δ_{K_v} を単に δ_v と書くことにする。Σ_K の任意の部分集合 $\mathcal{L}$ に対して、

$$\begin{aligned} S_{\mathcal{L},p^M}(E/K) &= \{c \in H^1(K, E_{p^M}) \mid \mathrm{res}_v(c) \in \delta_v(E(K_v)) \ \ \forall v \in \Sigma \setminus \mathcal{L}\} \\ &= \ker\left(H^1(K, E_{p^M}) \longrightarrow \prod_{v \notin \mathcal{L}} H^1(K_v, E)_{p^M}\right) \end{aligned}$$

とおく。$\mathcal{L} = \phi$ のときは $S_{p^M}(E/K) = S_{\mathcal{L},p^M}(E/K)$ と表わすことにする。このときよく知られているように

$$0 \longrightarrow E(K)/p^M E(K) \longrightarrow S_{p^M}(E/K) \longrightarrow Ш(E/K)_{p^M} \longrightarrow 0$$

は完全系列である。次の定理は定理 3.2 からすぐ出る。

Theorem 3.1 条件 (K)(M)(H)($G(p)$) の下で次が成り立つ。
(i) $p^{M_0} S_{p^M}(E/K)^{-\varepsilon} = 0.$
(ii) $p^{M_1}\left(S_{p^M}(E/K)^{\varepsilon}/\langle\delta(y_K)\rangle\right) = 0.$

Kolyvagin の証明の核心は $H^1(K, E_{p^M})$ の中に Euler system と呼ばれる非常に性質の良い元の系列を作ることにあった。それを定義するために、まず次の命題を示そう。

Proposition 3.2 P_n の $E(K_n)/p^M E(K_n)$ における類を $[P_n]$ で表わすと

$$[P_n] \in \left(E(K_n)/p^M E(K_n)\right)^{\mathcal{G}_n}.$$

(証明)[1], p.241 を参照。□

Proposition 3.3 条件 ($G(p)$) の下で制限写像 res : $H^1(K, E_{p^M}) \longrightarrow H^1(K_n, E_{p^M})^{\mathcal{G}_n}$ は同型である。

(証明)$E(K_n)_p = 0$ より明らか。□

次の図式を考えよう。

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E(K)/p^M E(K) & \xrightarrow{\delta} & H^1(K, E_{p^M}) & \xrightarrow{j} & H^1(K, E)_{p^M} & \longrightarrow & 0 \\ & & \downarrow & & \downarrow \mathrm{res} & & \downarrow \mathrm{res} & & \\ 0 & \longrightarrow & \left(E(K_n)/p^M E(K_n)\right)^{\mathcal{G}_n} & \xrightarrow{\delta_n} & H^1(K_n, E_{p^M})^{\mathcal{G}_n} & \xrightarrow{j_n} & H^1(K_n, E)_{p^M}^{\mathcal{G}_n} & & \end{array}$$

この図式を用いて $c_M(n) \in H^1(K, E_{p^M})$ と $d_M(n) \in H^1(K, E)_{p^M}$ を次のように定義する。

$$\begin{aligned} c_M(n) &= \mathrm{res}^{-1}\delta_n([P_n]), \\ d_M(n) &= j(c_M(n)) \end{aligned}$$

Kolyvagin は $\{c_M(n)\}_{n\in\Lambda(M)}$ を Euler system と呼んだ。但し、この notation は Gross による。

さて、$L(E/\boldsymbol{Q}, s)$ の関数等式の符号を $-\varepsilon = \pm 1$ とする。一般に $\mathrm{Gal}(K/\boldsymbol{Q})$-module X に対し、

$$X^{\pm} = \{x \in X \mid x^{\tau} = \pm x\}$$

とおく。ここで、τ は $\mathrm{Gal}(K/\boldsymbol{Q})$ の生成元である。

Proposition 3.4 $n \in \Lambda_r(M)$ に対し $\varepsilon_n = (-1)^r\varepsilon$ とおくと次が成り立つ。
(i) $c_M(n) \in H^1(K, E_{p^M})^{\varepsilon_n}$.
(ii) $d_M(n) \in H^1(K_n/K, E)^{\varepsilon_n}_{p^M} \subset H^1(K, E)^{\varepsilon_n}_{p^M}$.
(iii) $\mathrm{ord} d_M(n) \leq p^{M-M_r}$.
(iv) $\lambda \not| n$ ならば $d_M(n)_\lambda = 0$, $\lambda | n$ ならば $\mathrm{ord} d_M(n)_\lambda \leq p^{M-M_{r-1}}$.

Corollary 3.5 $n \in \Lambda_r(M_{r-1}+1)$ とすると次が成り立つ。
(i) $c_{M_{r-1}}(n) \in S_{p^{M_{r-1}}}(E/K)$.
(ii) $d_{M_{r-1}}(n) \in Ш(E/K)_{p^{M_{r-1}-M_r}}$.

(証明) Proposition 3.4 (iv) より

$$d_{N_{r-1}}(n)_v = 0 \qquad (\forall v \in \Sigma_K)$$

であることが判る。従って、$d_{M_{r-1}}(n) \in Ш(E/K)$。更に、同 (iii) より $d_{M_{r-1}}(n) \in Ш(E/K)_{p^{M_{r-1}-M_r}}$。よって (ii) が成り立つ。(i) は Selmaer 群の定義と (ii) より従う。□

$M_{r-1} > M_r$ であるときは、n を適当に選ぶと $Ш(E/K)$ の自明でない元が構成できるのであるが、実は $Ш(E/K)_{p^\infty}$ は $d_{M_{r-1}}(n)$, $n \in \Lambda_r(M_{r-1}+1)$ で生成されていることがわかるのである。

4 Theorem 1.5 の証明

Theorem 2.2 の証明は大変なのでここでは Theorem 1.5 の証明を（しかもその outline のみを）示すことにする。以下、簡単のため

$$S = S_{p^M}(E/K)$$

とおく。更に、$L = K(E_{p^M})$, $\mathcal{G} = \mathrm{Gal}(L/K)$ とおく。このとき、条件 $(G(p))$ の下では制限写像

$$H^1(K, E_{p^M}) \longrightarrow H^1(L, E_{p^M})^{\mathcal{G}} = \mathrm{Hom}_{\mathcal{G}}(\mathrm{Gal}(\overline{L}/L), E_{p^M})$$

は同型である。従って $S \subset H^1(K, E_{p^M})$ に対応して L の Galois 拡大体 L_S で

$$S \xrightarrow{\sim} \mathrm{Hom}_{\mathcal{G}}(\mathrm{Gal}(L_S/L), E_{p^M})$$

なるものが存在する。ここで $\delta(y_K) \in S$ より $L(p^{-M}y_K) \subset L_S$ である。以下、次の記号を用いる。

$$\begin{aligned} H &= \mathrm{Gal}(L_S/L), \\ I &= \mathrm{Gal}(L_S/L(p^{-M}y_K)). \end{aligned}$$

このとき、$H/I \cong (\boldsymbol{Z}/p^{M-M_0}\boldsymbol{Z})^2$ であるが、更に

$$(H/I)^+ \cong (H/I)^- \cong \boldsymbol{Z}/p^{M-M_0}\boldsymbol{Z}$$

である。

まず (i) を証明しよう。$\lambda \in \Lambda_1$ に対して λ の上にある L の素イデアルをひとつ選んで λ_L と表わしておく。このとき

$$\mathcal{L} = \{\lambda \in \Lambda_1(M) \mid \mathrm{Frob}(\lambda_L) \text{ generates } (H/I)^+\}$$

とおくとき、自然な写像

$$S^{-\varepsilon} \longrightarrow \prod_{\lambda \in \mathcal{L}} (E(K_\lambda)/p^M E(K_\lambda))^\varepsilon$$

は単射である。この dual をとって、全射

$$\bigoplus_{\lambda \in \mathcal{L}} ((E(K_\lambda)/p^M E(K_\lambda))^\varepsilon)^* \longrightarrow (S^{-\varepsilon})^*$$

を得る。ここで Tate duality より

$$((E(K_\lambda)/p^M E(K_\lambda))^\varepsilon)^* \cong H^1(K_\lambda, E)_{p^M}^{-\varepsilon} \cong \boldsymbol{Z}/p^M\boldsymbol{Z}$$

である。$\ell \in \Lambda_1$ を $\lambda = (\ell) \in \mathcal{L}$ となるようにとると、$d_M(\ell)_v = 0$ $(\forall v \neq \lambda)$ であるから $c_M(\ell) \in S_{\mathcal{L}}$ である。しかも

$$\mathrm{ord} d_M(\ell)_\lambda = p^{M-M_0}$$

であることが確かめられる。従って、我々は全射

$$\frac{\oplus_\lambda H^1(K_\lambda, E)_{p^M}^{-\varepsilon}}{\oplus_\lambda \langle d_M(\ell) \rangle} \longrightarrow \frac{\oplus_\lambda H^1(K_\lambda, E)_{p^M}^{-\varepsilon}}{\text{image of } S_{\mathcal{L}}^{-\varepsilon}} \longrightarrow (S_{\mathcal{L}}^{-\varepsilon})^*$$

を得るが、各 $\lambda \in \mathcal{L}$ に対して

$$\frac{H^1(K_\lambda, E)_{p^M}^{-\varepsilon}}{\langle d_M(\ell) \rangle} \cong \boldsymbol{Z}/p^{M_0}\boldsymbol{Z}$$

であるから $p^{M_0}(S^{-\varepsilon})^* = 0$。よって $p^{M_0}S^{-\varepsilon} = 0$。

次に、(ii) を証明しよう。$\ell' \in \Lambda_1(M)$ を

$$\begin{cases} \langle c_M(\ell') \rangle \cap S = 0 \\ \mathrm{ord} c_M(\ell') = p^{M-M_1} \end{cases}$$

となるようにとり fix して、$L' = L_{\langle c_M(\ell') \rangle}$ とおく。このとき、$\mathrm{Gal}(L'/L) \cong \boldsymbol{Z}/p^{M-M_1}\boldsymbol{Z}$ である。今度は $\mathcal{L}$ の代わりに

$$\mathcal{L}' = \left\{ \lambda = (\ell) \;\middle|\; \begin{array}{ll} \ell \in \Lambda_1(M) & \\ (\text{イ}) & \mathrm{Frob}(\lambda_L) \in I^+ \\ (\text{ロ}) & \mathrm{Frob}(\lambda_L)|_{L'/L} \text{ generates } \mathrm{Gal}(L'/L) \end{array} \right\}$$

を考える。このとき $\lambda = (\ell) \in \mathcal{L}'$ に対して（イ）より $c_M(\ell) = 0$, （ロ）より $\mathrm{ord} c_M(\ell')_\lambda = p^{M-M_1}$ となることが判る。更に、

$$\begin{cases} d_M(\ell\ell')_{\lambda'} = 0 \\ \mathrm{ord} d_M(\ell\ell')_\lambda = p^{M-M_1} \end{cases}$$

となる。従って、(i) と同様にして全射

$$\frac{\bigoplus_{\lambda'} H^1(K_\lambda, E)^\varepsilon_{p^M}}{\bigoplus_{\lambda'} \langle d_M(\ell\ell') \rangle} \longrightarrow (S^\varepsilon / \langle \delta(y_K) \rangle)^*$$

を得る。よって $p^{M_1}(S^\varepsilon / \langle \delta(y_K) \rangle) = 0$。□

参考文献

[1] Gross, B. H., Kolyvagin's work on modular elliptic curves, L-functions and Arithmetic, London Mathematical Society Lecture Note Series 153 (1991), 235-256.

[2] Gross, B. H. and Zagier, D., Heegner points and derivatives of L-series, Invent.Math. 84 (1986), 225-320.

[3] Kolyvagin, V. A., Euler systems, Grothendieck Festschrift, Prog. in Math., Boston, Birkhäuser, 1990.

[4] Kolyvagin, V. A., Finiteness of $E(\boldsymbol{Q})$ and Ш$(E/\boldsymbol{Q})$ for a class of Weil curves, Math.USSR Izvestiya 32 (1989), 523-541.

[5] Kolyvagin, V. A., On the Mordell-Weil and Shafarevich-Tate groups for Weil elliptic curves, Math.USSR Izvestiya 33 (1989), 473-499.

[6] Kolyvagin, V. A., On the structure of Shafarevich-Tate groups, Springer Lecture Notes in Mathematics,

[7] McCallum, W. G., Kolyvagin's work on Tate-Shafarevich groups L-functions and Arithmetic, London Mathematical Society Lecture Note Series 153 (1991),296-316.